North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Quick Links

North Dakota

Crash causes Guard base lockdown. Police and military officials said a man is accused of drunken driving after he crashed a car through the fence of the North Dakota Air National Guard base in Fargo, North Dakota September 29, sending the base into lockdown for about 2 hours. The Fargo Forum reports that the 59-year-old suspect was arrested late September 29
n suspicion of driving under the influence and driving with a revoked license. A Fargo police spokesman said the suspect's vehicle struck a tree, went through a fence and struck another tree on the base. He said the man got out of the car before it caught fire. The suspect was treated and released at a Fargo hospital and taken to the Cass County Jail. Source:
http://plainsdaily.com/story/6572

Regional

(Minnesota) **Charges: Man threatened to blow up Dairy Queen.** A 27-year-old man has been charged with terroristic threats and robbery after police said he used a bomb threat to rob a Dairy Queen September 20 in Rosemount, Minnesota. According to the criminal complaint, the suspect, who is homeless, allegedly entered the Dairy Queen on Canada Avenue and told employees he was going to blow up the place if he was not given money. Also, he allegedly told the employees that he was being forced to rob the business and that they should not call police until 3 minutes after he left. Rosemount police responded, and later located the suspect and a 23-year-old woman. They were taken into custody and separated. The pair told police that unknown individuals jumped into their car, threatened them with knives and guns and ordered them to commit the robbery, according to the complaint. Later, after more detailed interviews, police said their stories began to conflict. The suspect was charged with one felony count of first-degree aggravated robbery and one felony count of terroristic threats. If convicted, he faces up to 20 years in prison on the robbery charge, and 5 years in prison on the threats charge. Source:
http://wcco.com/crime/dairy.queen.robbery.2.1940667.html

(Minnesota) **International Falls CBP agriculture specialists intercept destructive pests.** U.S. Customs and Border Protection (CBP) agriculture specialists discovered potentially destructive pests September 8 at the rail facility in International Falls, Minnesota, the CBP announced recently. A container arriving from Bangladesh via Canada was targeted by CBP for an intensive agriculture examination for potential foreign pests. The shipment, destined for Chicago, Illinois was offloaded and the containers swept out. During the inspection of the pallets, a total of 14 live insects were intercepted and sent to the United States Department of Agriculture (USDA) for identification. USDA specialists identified two of the insects as a scaly cricket (Mogoplistrida sp.), and a gall midge (Xylodiplosis sp.), both actionable pests. These insects are detrimental to plant growth and development and may not occur in the United States. Gall midges are tiny mosquito-like insects that attack plant tissue and form galls in which their larvae develop. Scaly crickets are small crickets that can't fly, but eat the leaves of a wide variety of plant species. The shipment will be fumigated to

remove the pest threat before final distribution of the commodity into the United States. Source: http://www.ifallsdailyjournal.com/news/national-news/international-falls-cbp-agriculture-specialists-intercept-destructive-pests-109

(South Dakota) **Wildfire burns more than 400 acres in southwest SD.** A wildfire scorched more than 400 acres along the Cheyenne River just outside Badlands National Park in southwest South Dakota. No buildings were damaged and no one was hurt. KEVN said firefighters fought the blaze about 2 miles from Red Shirt on the ground and with a helicopter, and had it contained the afternoon of October 3. They plan to monitor the area for several days. Authorities believe hunters on all-terrain vehicles might have sparked the prairie fire. A Rapid City Fire battalion chief is urging hunters to be cautious when driving through grassy areas. Source: http://www.ktiv.com/Global/story.asp?S=13261874

(South Dakota) **Senator: Let rain-soaked farmers, ranchers plant emergency crops.** In South Dakota, too much rain is rarely a concern, but not the case this year, with rain records being set on a regular basis across the state. The wet year has soaked the financial status of many farmers and ranchers. A U.S. Senator introduced legislation September 29 that would assist farmers and ranchers who have been impacted by the soggy year. The legislation would ensure that producers who receive prevented planting benefits are able to plant a secondary crop — for emergency use only — without sacrificing any of their prevented planting assistance. “Given the enormous amount of rainfall, producers had fewer acres to plant this past spring and summer,” the senator said September 29. “In the future, my bill would allow producers to plant a second crop for emergency livestock feed without losing their prevented planning benefits.” Producers are not able to plant and access a second crop after receiving the benefits without losing 65 percent of their prevented planning compensation, and also an Actual Production History of 60 percent of the crop involved. Source: http://www.mitchellrepublic.com/event/article/id/46434/

(South Dakota) **Rains fall; Big Sioux explodes.** Relentless rain pounded Moody County, South Dakota, and caused some of the worst flooding seen in the area in years as well as damaging a lowhead dam in Flandreau. The rain swelled the banks of the Big Sioux River throughout the county, causing property damage, evacuations and road closures. A Moody County emergency manager said the Big Sioux River peaked at 13.67 feet and was at 12.45 feet as of September 27, according to a measurement taken at a location about 2 miles into the northern edge of Moody County. The river had been going down “gradually,” he said, and was still in major flood stage, which is 12 feet. The highest rainfall totals measured were in Egan, where 8 inches fell in a 2-day stretch Sept. 22-23. Almost 6 inches fell in Flandreau during that time period. The small community that is bordered to the west by the Big Sioux River was the hardest hit. Water levels at the park and Flandreau’s lowhead dam were much higher last week that during the flooding last spring. The dam was again flowing straight across, and the river flooded the road leading to Flandreau Indian School, which had been closed just beyond the bridge late last week. The Flandreau Public Works superintendent said the city will have to repair sections of the dam damaged during the flood. Source: http://www.moodycountyenterprise.com/v2_news_articles.php?heading=0&story_id=2196&page=73

National

Europe on alert after attacks warning. Japan October 4 became the latest country after Britain and the United States to issue a travel alert for its citizens amid growing fears of a major Al-Qaeda attack on landmark sites in Europe. The U.S. State Department said in its alert October 3 that attackers may use "a variety of means and weapons and target both official and private interests" in Europe. Fox News, citing unnamed intelligence officials, said militants had a list of targets in France and Germany, including Paris' Eiffel Tower and Notre Dame Cathedral, Berlin's Brandenburg Gate, the city's central railway station, and the Alexanderplatz TV tower. Fox cited a senior western intelligence official as saying that the information about the target list was provided by "a German-Pakistani national interrogated at Bagram Air Base in Afghanistan." The reports said well-armed teams of jihadists planned to seize and murder Western hostages in a manner similar to the attacks 2 years ago on two hotels and a railway station in the Indian city of Mumbai. Source: http://www.google.com/hostednews/afp/article/ALeqM5iGqj9wIc8I2y_jR5Y4MiJUMYERQw?docId=CNG.85334e3a27ad4bcf55b3f7bc6b1468a9.451

Mighty rains deluge cars, close roads in Northeast. Torrential downpours from a faded tropical storm inundated the Northeast October 1, forcing evacuations, toppling trees, cutting power to thousands and washing out roads during a snarled morning commute. Water pooled so deeply in a Philadelphia, Pennsylvania suburb that a car literally floated on top of another car. The storm that killed five people in North Carolina September 30 soaked a great swath of the Northeast by the October 1 morning commute, including New York City and Philadelphia. Flights coming into LaGuardia Airport in New York City were delayed 3 hours and traffic coming into Manhattan was delayed by up to 1 hour under a pounding rain. More than 26,000 power outages were reported in Connecticut, while New Jersey had just over 14,000 homes and businesses without electricity. North of New York City, about 8,000 customers in Westchester and Rockland counties had lost power, but many had been restored by mid-morning. Source: http://www.forbes.com/feeds/ap/2010/10/01/general-us-east-coast-storm_7977741.html

(Georgia) **Investigation into fatal gas explosion underway.** Some people who live near the site of a gas explosion that killed a Cairo, Georgia utility worker are still frightened. A leaking gas line in a residential area erupted into flames September 28. The state public service commission now said it could be months before investigators figured out what triggered the deadly blast. "It's not common," said a spokesman for the Georgia Public Service Commission (GPSC). "As far as pipelines, it's very unusual that we have an incident like this," he said. "I think the last explosion we had was in north Georgia back in the spring. But that was found to be an act of deliberate arson." The GPSC, which is in charge of regulating pipeline safety, is investigating the accident. Source: http://www.walb.com/Global/story.asp?S=13240320

(Alabama) **Gulf Coast copper thefts may be linked.** A man suspected of stealing copper from Fort Whiting in Mobile, Alabama may also be tied to thefts at Alabama Power and the University of South Alabama. Mobile police said their investigation began with a call from Fort Whiting August 30. Someone had stolen 2,500 feet of copper welding cable worth $3,000. No suspects were identified or arrested for the theft. Almost 1 month later, Fort Whiting called police again. On September 20, aluminum poles worth $4,500 were stolen. Mobile police identified the suspect in the September 20

theft. Investigators also checked scrapyards and found the same suspect had sold the welding cable stolen August 30. He was also believed to have stolen copper wire from Alabama Power. Police also learned the University of South Alabama was investigating the same suspect for stealing property from its Brookley campus. The FBI is also involved in the investigation, because Fort Whiting is federal property. The suspect is currently being held at the Mobile County Metro Jail on three counts of theft of property first degree. Source: http://www.fox10tv.com/dpp/news/local_news/mobile_county/fbi-involved-in-copper-theft-investigation

INTERNATIONAL

Pirate attacks at sea expanding. Although the U.S. government has made progress in implementing its 2008 Action Plan to combat piracy on the high seas, pirates have adapted their tactics and expanded their area of operations, almost doubling the number of reported attacks from 2008 to 2009, according to a new report from the Government Accountability Office (GAO). The report, titled Actions Needed to Assess and Update Plan and Enhance Collaboration among Partners Involved in Countering Piracy off the Horn of Africa, found that "although the Action Plan's objective is to repress piracy as effectively as possible, the effectiveness of U.S. efforts is unclear because the agencies implementing the plan are not tracking costs — such as operating ships and aircraft and prosecuting pirates — or evaluating the relative benefits or effectiveness of their actions. Thus, decisionmakers lack information that could be used to target limited resources to provide the greatest benefit, commensurate with U.S. interests in the region." "The United States has advised industry partners on self-protection measures, contributed leadership and assets to an international coalition patrolling pirate-infested waters, and concluded prosecution arrangements with Kenya and the Seychelles," the report states. Despite these collaborative efforts, however, the report notes that "from 2007 to 2009, the most recent year for which complete data were available, the total number of hijackings reported to the International Maritime Bureau increased, ransoms paid by the shipping industry increased sharply, and attacks spread from the heavily patrolled Gulf of Aden — the focus of the Action Plan — to the vast Indian Ocean." Source: http://www.hstoday.us/content/view/14933/149/

Mexican military crosses into US side of Progreso bridge. The Progreso International Bridge was closed down for a short time October 1 following an incident with the Mexican military. The Mexican military members were allegedly chasing a speeding driver of a Dodge Nitro SUV. The driver crossed from the United States into Mexico. At the Mexican checkpoint, the driver turned around and fled back to the United States. The Mexican military followed and crossed the international boundary on the bridge. As a result, the Progreso International Bridge was temporarily shut down on both sides. A U.S. Customs and Border Protection (CBP) spokesman said they spoke to the military and informed them that they crossed the line. He said CBP consider the crossing unintentional. Everything was back to normal and traffic was flowing again the evening of October 2. Source: http://www.krgv.com/news/local/story/Mexican-Military-Crosses-into-US-Side-of-Progreso/viinSCdTT02RJZTOEYh5kw.cspx

Iran: Nuclear delay due to leak, not computer worm. A months-long delay in starting up Iran's first nuclear power plant is the result of a small leak, not a computer worm that was found on the laptops of several plant employees, the country's nuclear chief said October 4. The leak occurred in a storage pool where the plant's fuel is being held before being fed into the reactor core, and it has been fixed, said Iran's vice president. He did not specify whether it was nuclear fuel or another material that

leaked. He first announced the delay September 29 but without giving a reason. Iranian officials said they are vigorously battling the Stuxnet computer worm. Though it infected several personal computers of workers at the Bushehr plant, Iran said the facility's main systems were not affected. Source: http://www.google.com/hostednews/ap/article/ALeqM5iRqjZV1Meppj40hTs8IBOv4DdsQwD9IKSRK00?docId=D9IKSRK00

(Vermont) **Russians seek to learn about shutdown of nuke plants.** Last year several Russian delegates visited New England to witness what decommissioning a nuclear power plant is all about. With the help of the New England Coalition technical adviser, nearly a dozen delegates will return to tour Vermont. "They use the term decommissioning as an entire process," the technical advisor said. "They look at how to handle it from every angle, economics, the clean-up and the political interactions." During the week, the delegation will have the opportunity to speak with numerous organizations about what the decommissioning process looks like in the United States versus Russia, said a New England Coalition board member. Source: http://www.reformer.com/localnews/ci_16222443

Malta-flagged ship escapes attack off Tanzania. Pirates on September 28 attacked a chemical product tanker in Tanzanian waters as it was sailing to the commercial capital Dar es Salaam, but the ship managed to escape, the European Union's anti-piracy naval force said. The attack on the 13,054 dwt Malta-flagged MV Mississippi Star, with 18 crew members, was the second such incident in the waters of the East African state in 3 days. On September 26, Tanzania's navy captured a suspected Somali pirate after a gun battle 70 nautical miles off the southern Mtwara coast, an area where London-based, Africa-focused oil and gas firm Ophir Energy has an exploration vessel. The naval force said a nearby talian warship, the Libeccio, went to the scene and was monitoring the situation, and the Tanzanian navy had been alerted. Source: http://www.reuters.com/article/idUSLDE68R11P20100928

Towns south of Berlin evacuated after highest flood-alarm level imposed. Floodwaters from the rainiest September on record in eastern Germany forced the evacuation of at least 2,500 people in towns south of Berlin and closed schools and hospitals along the Elbe and Spree rivers. Authorities in Brandenburg imposed the highest level of alarm for flooding in the southern part of the state. This month has been the rainiest on record in eastern Germany. About 1,000 people are piling up sandbags to shore up dikes, and in some regions travel is being restricted. In Saxony, which borders the Czech Republic and Poland, water levels were expected to peak by October 1 in Dresden, according to the state's environment ministry Web site. Three people drowned in a basement in the town of Neukirchen less than 2 months ago following heavy flooding in Germany, the Czech Republic and Poland. Source: http://www.bloomberg.com/news/2010-09-30/germany-evacuates-towns-south-of-berlin-after-record-breaking-rainfall.html

Purported Europe terror plot called 'credible'. Threats of a possible "Mumbai-style" terror attack on Western interests in Europe are considered "credible" and U.S. officials are not ruling out the possibility that the plot could extend to the United States, a senior U.S. counterterrorism official told NBC News. One coalition official with access to intelligence reporting, which came from human sources as well as electronic intercepts, suggested possible attacks on hotels or other public gathering spots in a "fedayeen-style" commando attack by at least 25 operatives, much like the

devastating coordinated assault in Mumbai in 2008. The official said information about a possible plot emanating from al-Qaida-linked groups in northwest Pakistan was first picked up by U.S. intelligence several weeks ago and was believed to be aimed at targets in France, Germany or the United Kingdom. There is no evidence the alleged plot has been disrupted. "No one is assuming the threat has subsided," the U.S. official said. U.S. intelligence analysts are divided over how alarming the current threat reporting is, and some officials emphasized they have no "specific" information to suggest an attack is imminent — or that the United States is being targeted. Source: http://www.msnbc.msn.com/id/39413455/ns/world_news-europe/

Failed bank heist in Baghdad leaves 3 dead. A gang using bombs and automatic weapons tried to storm a bank in southwestern Baghdad in Iraq, in a failed robbery September 30 that officials said left three people dead, including two policemen. Police said the assault began with four bombs exploding near the state-run Al-Rafidain bank. In the ensuing gunbattle, two policemen and a bystander were shot dead. Two of the robbers were captured. Police and hospital officials said a total of six people were wounded, including three policemen. An Iraqi military spokesman said it was unclear whether the gang had political links or was purely criminal. Source: http://news.yahoo.com/s/ap/20100930/ap_on_re_mi_ea/ml_iraq

Europe terror threat still active. European security officials said September 29 a terror plot to wage Mumbai, India-style shooting sprees in Britain, France, and Germany is still active and that sites in Pakistan — where the threat was intercepted 2 weeks ago — are being scoured for al-Qaeda operatives. The plot was still in its early stages and not considered serious enough to raise the current terror threat level, officials said. Still, the Eiffel Tower in Paris, France was briefly evacuated September 28 for the second time in the past week because of an unspecified threat, and police were on alert in Britain and France. "This plot was in its embryonic stages," a British government official told the Associated Press September 29. "This one has preoccupied us more than others in the past few weeks — and it is still active — but it has not raised enough alarms to change our security threat level." The announcement of the plot came ahead of the September 30 anniversary of the Prophet Muhammad cartoons being published in a Danish newspaper. It also came as Spanish authorities announced they had arrested September 28 a U.S. citizen of Algerian origin on suspicion of financing al-Qaeda's North African affiliate. Source: http://www.google.com/hostednews/ap/article/ALeqM5glNGJLYipcY1gxBiWju9qrOz4ZbwD9IHKES80?docId=D9IHKES80

Gunmen steal weapons from police complex in Mexico. Gunmen broke into a police complex in northern Mexico September 27 and stole at least 40 automatic rifles and 23 handguns, authorities said. A Chihuahua state police spokesman said the assailants subdued several officers guarding the state police offices in Chihuahua city and forced them to show the way to the armory. The 10 officers who were in the building at the time are being questioned. He said it is not clear whether the assailants are members of a drug cartel. Source: http://www.google.com/hostednews/ap/article/ALeqM5gMi5B2USfJStXxfqgWWr2xjRYpOgD9IGFFUG2?docId=D9IGFFUG2

U.K. arrests 19 for major bank hack. Police arrested 19 people in London as part of an investigation into an international cybercrime gang that authorities believe stole at least $9.5 million from accounts held at major U.K. banks, including HSBC Holdings PLC and Royal Bank of Scotland Group

PLC. In dawn raids September 28, officers arrested the 15 men and 4 women on suspicion of computer-related crimes, according to London's Metropolitan police service, known as Scotland Yard. A police spokesman said they are not believed to be British citizens, but declined to specify their nationalities. Police suspect the group of having targeted thousands of computers belonging to U.K. banking customers by infecting them with a computer code called Zeus, which has become widely used by criminals world-wide. The code allowed the fraudsters to capture personal log-in details by enabling them to trick people who bank online into entering their details into fake Web pages that mimic those of their banks. Police believe the group then used the information to gain unauthorized access to the bank accounts and transfer funds to "mule" or "drop" accounts controlled by the criminal network. Source:
http://online.wsj.com/article/SB10001424052748704116004575521300419639946.html

French police dismantle mobile phone hacking ring. French police busted a network of mobile phone hackers, a fraud worth millions of euros, and arrested nine people, including employees of cellular phone companies, investigators said September 26. Three people were still in custody September 26 following the arrests across the country that came after a year-long investigation into the network, which had been operating for a decade and is the first of its kind in France, according to officials in an investigative unit of the Marseille gendarmerie. Investigators explained that fraudsters purchased codes to unlock SIM cards for $4 each from high-ranking phone company employees, who had access to company databases. The network subsequently sold the codes on the Internet for $40. The money earned from these sales were put into tax-free overseas bank accounts. With the codes, individuals could access any SIM card, even foreign cards, with their mobile phones. The investigation began at the end of 2009 after a complaint at French phone company SFR in the southern city of Marseille about discrepancies in its security system. Two other companies, Bouygues Telecom and Orange, were also affected by the fraud. Source:
http://www.google.com/hostednews/afp/article/ALeqM5jsQg3o74Kx_0QvOzWKs0r4Ppz_Vg

Banking and Finance Industry

Hackers siphoned $70 million. An international computer-crime ring that was broken up this week siphoned about $70 million in a hacking operation targeting bank accounts of small businesses, municipalities and churches, the FBI said October 1. FBI officials provided new details of a broad probe that included the arrests earlier in the week of people allegedly involved in a network of "mules," those recruited to move stolen funds via bank accounts opened with fake names. Authorities in the U.S., U.K., the Netherlands, and Ukraine have detained or charged more than 100 people. According to the FBI, the organization running the hacking ring included computer-code writers in Ukraine, and the mule-network operators spread out in the U.S., U.K., and Ukraine. Victims were mostly in the U.S., though some bank accounts were also targeted in the U.K., the Netherlands, and Mexico. Thieves using iterations of the Zeus computer program managed to steal hundreds of thousands of dollars at a time — the result of focusing on business accounts instead of individual consumers, the FBI said. Investigators said the transactions attempted could have led to losses of up to $220 million, but many were
not completed. Source:
http://online.wsj.com/article/SB10001424052748704029304575526393770024452.html?mod=googlenews_wsj

Money mule arrests highlight banks' efforts to fight fraud. The indictments unveiled last week against dozens of people who allegedly helped loot millions of dollars from U.S. businesses via online corporate account takeovers highlights the struggle by financial firms to fight fraud. Over the past 2 years, corporate account takeovers by cybercriminals have cost U.S. businesses more than $100 million, according to FBI estimates. In most cases, the thefts have been perpetrated by gangs in Eastern Europe who used the Zeus banking Trojan to break into computers belonging mainly to small businesses and small municipalities. The malware has been used to steal online banking credentials and access corporate accounts so the thieves could transfer money into fraudulent accounts set up by hundreds of U.S.-based accomplices, often called "money mules." Most of the illegal transfers were unauthorized Automated Clearing House (ACH) transactions from the victim's account to the money mule. The U.S Attorney's Office in New York City said September 30 it had indicted 37 such money mules for helping crooks based in Russia and several East European countries siphon off more than $3 million in stolen funds. In a joint announcement, Manhattan's District Attorney announced indictments against another 36 people for their participation in a similar operation. Source: http://www.computerworld.com/s/article/9189201/Money_mule_arrests_highlight_banks_efforts_to_fight_fraud

US banks and regulators 'fail' to cut money laundering. One of the United States' top fraud investigators is warning that America's policing of money laundering is wide open to abuse. He said that billions of dollars are slipping through the U.S. banking system. In testimony ahead of a Congressional hearing on terrorist financing September 28, he said that only international action can stop the laundering. The U.S. Committee on Financial Services is taking evidence on "trends in terrorism financing." The fraud investigator said the "powerful tools" to stop the laundering of drug and terrorist money "are not being used as vigorously and consistently as they could be" and that only the United States "possesses the resources and tools to protect the global financial system." He also criticized Wall Street' s due diligence. Another expert witness in his pre-hearing testimony said the problem was U.S. banks rely heavily on the accuracy of transactional information given to them by foreign banks. But very often U.S. banks have to take that information on trust, he said. Source: http://www.bbc.co.uk/news/business-11426166

Organizations struggling with PCI compliance. Security experts have used the September 30 Payment Card Industry Data Security Standards (PCI DSS) compliance deadline to warn against complacency in the industry. However, an international senior vice president at endpoint security firm Lumension suggested that the standard had left even the largest merchants confused. "PCI compliance might have been around for some time, but merchants are still struggling to get their heads around the requirements," he said. "Version 2.0 is just around the corner, meaning that merchants need to be concerned about their ability to prove compliance with v1.2, and with the steps they must take to get to the next stage of compliance. All too often, organizations fall into the compliance trap and focus all their efforts on meeting the requirements of a new deadline without thinking about the bigger picture," he said. "Taking a myopic view of regulatory compliance creates a situation where merchants are constantly reinventing the wheel, wasting time and effort, and ultimately blowing security budgets." Source: http://www.v3.co.uk/v3/news/2270762/organisations-struggle-pci

Zeus botnet thriving despite arrests in the U.S., U.K. The Zeus botnet remains a robust network that is difficult to destroy despite an international sting operation that saw dozens arrested the week of

September 27 for allegedly stealing money from online bank accounts. While it is encouraging to see law enforcement investigate, Zeus is still a problem, said a co-founder of the Shadowserver Foundation, an organization that tracks botnets. The arrests appear to not have had a significant technical impact on the Zeus botnet. As of October 1, at least 170 C&Cs for Zeus are still online, according to statistics compiled by the administrator of Zeus Tracker. On October 1, the Zeus tracker shows that the Russian registrar Reg.ru sold 10 domain names that are now being used for Zeus-related activity. Seven of those domain names are redirecting to one domain that recently hosted Zeus files. The most recent domain name sold through Reg.ru was added to Zeus Tracker September 29. That server temporarily hosted two kinds of Zeus files that have since been removed. It is possible that the owner of that domain discovered the infection and then removed the offending files. Source: http://www.computerworld.com/s/article/9189123/Zeus_botnet_thriving_despite_arrests_in_the_U.S._U.K.

PayPal plugs mobile site phishing risk. PayPal has fixed a cross-site scripting problem on its mobile payments site that, left unaddressed, had the potential for misuse in phishing attacks. The vulnerability, discovered by hacking and security site Security-Shell, also created a possible mechanism for hackers to redirect surfers from mobile.paypal.com onto untrusted sites. In a statement issued September 29, PayPal said it had plugged the Web site vulnerability. Source: http://www.channelregister.co.uk/2010/09/30/paypal_mobile_xss_plugged/

(Arizona) **Device detonated at bank near Anthem following robbery.** A bomb scare took place outside a bank near Anthem, Arizona September 24. Workers at a Bank of America witnessed a robbery and a bomb scare just before closing at the location on Daisy Mountain and Gavilan Parkway. Police said a man walked into the bank and handed a note to the teller demanding money. The suspect also told the teller there was a bomb outside. Workers immediately called 911, and Maricopa County deputies found a small device left on the front door of the bank when they arrived at the scene. The bomb squad detonated the device. Authorities said they are still not sure what th3 device was. The suspect remains at large. Source: http://www.azfamily.com/news/local/Bomb-scare-after-robbery-outside-bank-near-Anthem-103768609.html

6 tips for guarding against rogue sys admins. The vice president of the fraud program at the BITS Financial Services Roundtable said there has been an increase in insider incidents among U.S. financial services firms. “You have intentional breaches like theft of financial or propriety information and placement of logic bombs and malware, but you also have the unintentional breaches caused by insiders such as employees accidentally opening an infected file, installing unauthorized software or threats from social media,” the vice president said. “We’ve seen an increase in the intentional and the unintentional” insider-related security breaches. Network World spoke with CISOs and IT security experts about what practical steps IT departments can take to minimize the insider threat. Their advice is: Restrict and monitor users with special privileges; Keep user access and privileges current, particularly during times of job changes or layoffs; Monitor employees found guilty of minor online misconduct; Use software to analyze log files and to alert when anomalies occur; Consider deploying data-loss prevention technology; and educate employees about the insider threat. Source: http://www.computerworld.com/s/article/9188145/6_tips_for_guarding_against_rogue_sys_admins

Chemical and Hazardous Materials Sector

Audit: Changes needed to make nuke plants secure. A federal audit set to be released October 4 calls for the Nuclear Regulatory Commission (NRC) to improve nuclear power plant security against infiltration by potential terrorists. An outline of the findings was provided to the Associated Press by a U.S. Senator from New York. The Senator had called for the audit by the NRC's inspector general in March after a suspected al-Qaida member was found to have worked in a New Jersey nuclear power plant for 6 years. The audit recommends additional training in identifying suspected terrorists, greater access to criminal databases by the NRC, stepped up "re-screening" of power plant employees, and notifying plant operators of foreign travel. The Senator said the recommendations must be acted upon within 30 days. Source: http://www.google.com/hostednews/ap/article/ALeqM5jtsGK87a9gVLMl-e_OkaDHEE7gNAD9IKTCA00?docId=D9IKTCA00

Scientists: NRC fails to protect public. In the past several months, leaks of radioactively contaminated water have been discovered at three nuclear power plants in the northeastern part of the United States. According to a report released September 29 by the Union of Concerned Scientists (UCS), the Nuclear Regulatory Commission (NRC) has failed to protect the public. A safety advocate for UCS who assisted with the report, said the NRC has ignored more than two dozen violations since 2006. "NRC's enforcement record was spotty before 2006," the safety advocate said. "But since then, the agency has given power plants a free pass when it comes to leaking radioactively contaminated water." A dozen cases are reviewed in detail in the report, he said, including some where the NRC enforced its rules and how that changed the plant owner's response. The severity of the leak played no role in determining whether there was a sanction or the severity of the sanction. "The NRC might as well have based its decision on whether to enforce ... by spinning a roulette wheel," the safety advocate said. "There is a three-way contract among the NRC, plant owners and the public. The NRC honors its contract with plant owners by never demanding higher safety levels, but breaks its contract with the public by repeatedly accepting much lower safety levels." Source: http://www.reformer.com/localnews/ci_16222441

Commercial Facilities

(New York) **Suspicious package scare on Park Boulevard.** The Park Boulevard business district in Massapequa Park, New York, had to be evacuated for more than 2 hours September 30 after somebody left a suitcase unattended in front of a Subway sandwich shop. The owner of the Subway said he noticed the suitcase outside during the afternoon, but did not think anything of it until a customer suggested they check it at around 8:30 p.m. "He opened the zipper a little, and he saw an ID tag and some small parts," he said. "I told him, 'Don't touch it, it could be dangerous.' " He called police who immediately evacuated dozens of people from the shops and restaurants in the area. The Nassau County police bomb squad was summoned and determined the suitcase was harmless and only contained someone's personal belongings, police said. Park Boulevard was closed between Sunrise Highway to Clark Boulevard for about 2 hours. Source: http://massapequa.patch.com/articles/suspicious-package-scare-on-park-boulevard

(Illinois) **Pipe bomb death a suicide.** Police have determined that the 21-year-old man who died in a pipe-bomb explosion September 14 in a park in Evanston, Illinois, 2 weeks ago committed suicide and had no plan to hurt others. Police found information on his computer that revealed he had been researching methods of making a bomb, and evidence as to the place and time he selected to detonate the bomb showed that he intended only to kill himself. Additionally, a suicide note was found by police. Source: http://www.suntimes.com/news/metro/2760262,CST-NWS-explosion30.article

(New York) **Times Square bomber targeted largest crowds.** Federal prosecutors said the man convicted of trying to set off a car bomb in Times Square May 1 regularly checked live video feeds to see where, and at what time, the crowds would be the largest. In a memorandum filed September 29 urging a federal judge to sentence the man to life in prison, prosecutors said he told the FBI after he was arrested that believed the car bomb would have killed at least 40 people. If he had not been arrested, he told the FBI, he planned to build and set off another car bomb somewhere in New York City 2 weeks later. The government said he left the United States in 2009 for the explicit purpose of learning to build a bomb and attack U.S. targets. While there, he made a video which was released by the Taliban in July of this year. On it, he said, "I have been trying to join my brothers in jihad since 9/11 happened. I am planning to wage an attack inside America." Source: http://www.nbcsandiego.com/news/breaking/NBC__Times_Square_bomber_targeted_largest_crowds-104021598.html

(Texas) **Police retrieve active pipe bomb from a parking lot.** Authorities in Corpus Christi, Texas, found two pipe bombs September 29, at least one of which they believe was active, in a car parked in a crowded grocery store lot. The owner of the car was arrested, and a crew of agents from the Houston office of the Bureau of Alcohol, Tobacco and Firearms was sent to retrieve and dismantle the device, officials said. Police wouldn't speculate how much damage an explosion at the H-E-B in the 5900 block of Weber Road would have caused. "If it's got the ability to go 'boom,' it's got the ability to seriously injure or kill," said a captain of the Corpus Christi Police Department. About 8 a.m. the 35-year-old suspect called police to report a verbal disagreement with another man in the parking lot. When officers arrived, he gave police permission to search his 2010 Toyota Yaris, in which they found a rifle and what looked like two pipe bombs, officials said. The suspect was arrested on suspicion of felony possession of a prohibited weapon. He is being held in the Nueces County Jail on $75,000 bail. Source: http://www.caller.com/news/2010/sep/29/police-retrieve-active-pipe-bomb-from-a-parking/

(Connecticut) **Supermarket searched due to bomb threat.** Stop & Shop supermarkets in several Connecticut communities were the targets of a bomb threat September 29. The threat was made around 10:32 a.m. during a 911 call from an untraceable cell phone received by dispatchers at State Police Troop G in Bridgeport. The caller stated that a Stop & Shop supermarket in Bridgeport, Fairfield, Stratford, Milford, Trumbull or Wilton, or the Osborn Correctional Center, would blow up at roughly 11:50 p.m, according to a Stratford police captain. Stratford police conducted a walkthrough of the Stop & Shop at East Main Street, in the Dock Shopping Center, but the store was not evacuated. Fire and EMS units also responded after a threat concerning that store was received. Nothing was found, however, and state police said the incident is still under investigation. In February, a Stop & Shop employee was charged with committing an act of terrorism when he allegedly made an early morning bomb threat that closed the supermarket on Monroe Turnpike.

Source: http://www.ctpost.com/news/article/Supermarket-evacuated-due-to-bomb-threat-679604.php

(California) **Petaluma explosion could be linked to pipe bomb.** A resident who was walking near Wiseman Park in Petaluma, California, September 26 found an 18-inch-long, 2-inch-wide metal pipe that appeared to have been used as an explosive device. The pipe was found in weeds on the edge of the park. An explosion that reverberated through part of Petaluma September 24 is perhaps linked to the discovery. Numerous residents contacted police over the weekend to report hearing and feeling the explosion. It is unknown if the pipe was connected to the previous explosion, police said. Source: http://www.pressdemocrat.com/article/20100927/articles/100929531

(District of Columbia) **Suspicious package found near Nats Park.** Traffic in the vicinity of Nationals Park, the stadium where the Washington Nationals of Major League Baseball play in Washington D.C., was disrupted September 27 after a suspicious package was discovered in the area. Authorities investigated the package using X-ray equipment, then removed the packaged. The incident occurred near the Navy Yard train station on the Washington Metropolitan Area Transit Authority Green Line, which is one of the main means of access to the stadium. One entrance of the station was reported closed. Source: http://voices.washingtonpost.com/local-breaking-news/crime-and-public-safety/suspicious-package-found-near.html

(Indiana) **Possible sticks of dynamite explode in trash in LaPorte County.** Two apartment buildings containing 15 units in Michigan City, Indiana were evacuated September 27 after a quarter-stick of dynamite blew up as a garbage truck was emptying a dumpster into the trash compactor. It was the first of two explosions caused by quarter-sticks of dynamite thrown into the trash. According to police, the first explosion occurred at Normandy Village Apartments about 10:30 a.m. as the truck with its mechanical arm was emptying the dumpster. Police said the garbage truck was rocked but not damaged. After that explosion, the garbage hauler made the 30-minute trip back to the Waste Management-owned transfer station at the Kingsbury Industrial Park in Kingsbury to examine the contents of the compactor to try and find out what caused the blast. As the contents were being dumped out, there was another much more powerful blast that shattered lights and a windshield on a payloader, and knocked a bathroom sink off the wall, police said. That blast prompted an emergency response back to Normandy Village where the apartment buildings were evacuated and the area sealed off for 4 hours as a precaution. Recovered from the trash was a paper bag containing roughly 50 gunpowder-filled cylinders roughly 3 to 4 inches long and 1 inch in diameter. The source of the illegal explosives was still being investigated. Source: http://www.wsbt.com/news/local/Possible-sticks-of-dynamite-explode-in-trash-in-LaPorte-County--103903344.html

Communications Sector

(South Carolina) **Copper thieves cause major damage during heist in Rock Hill.** Police in South Carolina are looking for suspects responsible for a copper theft that caused $200,000 worth of damage to a York County Communications tower in September. The Rock Hill Police Department said thieves stole $1500 worth of copper from the tower in the 1800 block of Canterbury Glen in Rock Hill, sometime between September 9 and September 29. An employee was making a monthly inspection of the tower when he discovered the damage. This investigation is ongoing. Source: http://www.wbtv.com/Global/story.asp?S=13252869

Verizon to issue refunds to 15 million customers. Verizon Wireless in a statement October 3 said it will pay up to $90 million in refunds to 15 million cell phone customers who were erroneously charged for data sessions or Internet use. Verizon said 15 million customers either will receive credits of $2 to $6 on their October or November bills, while former customers will get refund checks. The charges affected customers who did not have data usage plans, but were billed because of exchanges initiated by software built into their phones. In the past 3 years, the U.S. Federal Communications Commission (FCC) received complaints from Verizon Wireless customers who said they were charged for data usage or Web access, the New York Times reported October 3. People close to the settlement talks said they expected the refunds to total more than $50 million, the Times said. These people also said the FCC is pressing Verizon to agree to a penalty for the unauthorized charges. Source: http://www.msnbc.msn.com/id/39491340/ns/business-us_business/

Increase in VoIP attacks prompts expert to build specialized blacklist. Overwhelmed by the number of attacks against PBX systems at the managed service provider where he works, a security engineer has launched a project to gather and and list offending Internet Protocol (IP) addresses involved in VoIP abuse. “Throughout the course of the day, I got tired of seeing VoIP-based brute force attempts that I decided to out companies who sit around and choose to do nothing about the attacks coming from their networks,” the initiator of the VoIP Abuse Project said. “In an effort to make other companies who have PBX servers online aware of the attackers, I will be posting the information of address and companies [from] which these attacks are coming from,” he said. The term PBX stands for private branch exchange and refers to the multi-line telephone systems used in business environments. Attackers hack into such systems to make long-distance calls to foreign countries or launch over-the-phone phishing attacks known as vishing. According to him, the most common type of attack he sees is brute forcing and comes from systems that have already been compromised. Source: http://news.softpedia.com/news/Increase-in-VoIP-Attacks-Prompts-Expert-to-Build-Public-Blacklist-158870.shtml

Report: U.S. would make Internet wiretaps easier. The U.S. President’s administration is pushing to make it easier for the government to tap into Internet and e-mail communications. But communications firms may be wary of its costs and scope. Frustrated by sophisticated and often encrypted phone and e-mail technologies, U.S. officials said law enforcement must improve its ability to eavesdrop on conversations involving terrorism, crimes or other public safety issues. Critics worry the changes might make citizens and businesses more vulnerable to identity theft and espionage. The new regulations that would be sent to Congress in 2011 would affect American and foreign companies that provide communications services inside the U.S. It would require service providers to make the plain text of encrypted conversations — over the phone, computer or e-mail — readily available to law enforcement, according to federal officials and analysts. Source: http://news.yahoo.com/s/ap/us_internet_wiretaps;_ylt=Aqu25DccBH64QmMR8cCdS82s0NUE;_ylu=X3oDMTNscnR1cmQwBGFzc2V0A2FwLzIwMTAwOTI3L3VzX2ludGVybmV0X3dpcmV0YXBzBGNjb2RlA21vc3Rwb3B1bGFyBGNwb3MDMwRwb3MDMTEEcHQDaG9tZV9jb2tHNlYwN5bl90b3Bfc3RvcnkEc2xrA3JlcG9ydHVz

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

AIA issues report on health of national security space industrial base. The national security space industrial base faces a tipping point beyond which irreparable harm to the U.S. defense and economy could occur, according to a new report released by the Aerospace Industries Association (AIA). "Our national leaders, the military and our economic well-being all rely on our space assets more than at any point since the dawn of the space age," said the AIA President and CEO. The report, Tipping Point: Maintaining the Health of the National Security Space Industrial Base, laid out several challenges faced by the national security space industrial base, including overly restrictive export control policies, a shrinking, aging workforce, and budget instability. "Other nations are making rapid advancements in acquiring or exploiting space capabilities," the CEO said. "America's leadership in space is no longer guaranteed." AIA made several policy recommendations to address the challenges facing government and industry. Source: http://www.spacemart.com/reports/AIA_Issues_Report_on_Health_of_National_Security_Space_Industrial_Base_999.html

(Florida) **Defense contractor confirms indicted Florida businessman sold counterfeit computer chips.** Federal authorities said a Pinellas County, Florida businessman for years dealt in counterfeit computer chips, risking the lives of military personnel and potentially endangering national security. Authorities said his dealings in counterfeit "military grade" integrated circuits, or ICs, made him rich, but one alleged victim — a major defense contractor specializing in missile technology — said the company purchased chips that turned out to be fake from a supplier, who bought them from the businessman. "We quickly determined upon failure-testing they were counterfeit and contacted the FBI," said a spokesman for Raytheon, a major defense and aerospace systems supplier. The week of September 13, federal authorities descended on the businessman's Clearwater electronics dealership, VisionTech Components, after a Washington D.C. grand jury came back with indictments for him and his office manager accusing them of mail fraud and trafficking in counterfeit goods. U.S. Attorney's Office officials said his company made 31 separate sales of 59,540 counterfeit integrated circuits imported from China and Hong Kong for $425,293 to various companies, including ones with contracts with the U.S. Navy. Source: http://floridaindependent.com/8706/defense-contractor-confirms-indicted-florida-businessman-sold-counterfeit-computer-chips

(Texas) **Pantex begins disassembly of a W84 warhead.** The National Nuclear Security Administration (NNSA) September 29 announced it has completed disassembly and inspection of the first W84 at NNSA's Pantex Plant in Amarillo, Texas. This marks the beginning of the disassembly and inspection process for the W84, a thermonuclear warhead that entered the stockpile in 1983. The process will confirm the system, which has not been disassembled since 1998, has not experienced safety-related aging issues. The project team consisting of members from NNSA, Lawrence Livermore National Laboratory, Sandia National Laboratories in California and Pantex worked together for 24 months and completed the project ahead of schedule. "Disassembly and inspection of this system allows us to

look at its components to find out how the weapon has aged," said NNSA's Deputy Administrator for Defense Programs. "This analysis helps us maintain a safe, secure and effective stockpile without the need for nuclear testing. The scientific and technical knowledge we gain when we disassemble a weapon is invaluable as we look across all of our systems." Source: http://www.yourindustrynews.com/pantex+begins+disassembly+of+a+w84+warhead_54644.html

GE-Rolls examines F136 after fan problem. General Electric and Rolls-Royce are focusing on manufacturing records as they investigate the causes of an incident that forced the shutdown of a F136 development engine September 23. The shutdown was triggered when the F136 endurance engine, 008, "experienced an anomaly at near-maximum fan speed," the GE-Rolls Fighter Engine Team said. "Initial inspection revealed damage to airfoils in the front fan and compressor area. The engine is currently being disassembled for a thorough investigation," it added. The test incident comes at a potentially perilous time for the F136, which is once again struggling for survival in the continued debate in Washington D.c. over funding for the F-35 Joint Strike Fighter alternate engine. The U.S. President has promised to veto any bill prolonging the F136, although the House of Representatives already is on record challenging the threat. The issue is likely related to an assembly or set-up problem linked to this specific engine rather than a deeper, systemic failure. Although GE-Rolls is not commenting on specific focus areas, the statement points to the front fan in the Rolls-Royce-led fan module as being the chief suspect. Source: http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awx/2010/09/28/awx_09_28_2010_p0-257899.xml

Emergency Services

(Oklahoma) **Man arrested for shooting Oklahoma City police helicopter.** Tips from Crime Stoppers helped Oklahoma City, Oklahoma officers recently arrest a man suspected of shooting at the Air One Police Helicopter. Police noticed a bullet hole in Air One June 28 during a preflight inspection. They believed the aircraft was shot the night before during its routine patrol. Pilots said they did not notice the shot during their flight. A tip from the Crime Stoppers hotline led police to an 18-year-old suspect. Police believed he was the person who shot at Air One. He faced charges of assault with a deadly weapon and possession of a firearm in committing a felony. The suspect has been booked into the Oklahoma County Jail. Source: http://www.news9.com/Global/story.asp?S=13238878

(California) **Suspicious envelope prompts evacuation of LAPD station; substance determined harmless.** An envelope containing white powder prompted a hazardous-materials response at the Los Angeles Police Department's Rampart Station in Los Angeles, California September 28, but the substance turned out to be harmless. The scare was reported shortly before 1 p.m., with about 10 people believed to have been exposed. Police initially had little to say about the scare, which came in the wake of demonstrations over the officer-involved shooting death of a Guatemalan day laborer, but did send an LAPD spokeswoman to the station at 1401 Sixth St. An LAPD spokersperson said it was not known whether the envelope was mailed to the station. A police sergent later confirmed the substance was talcum powder. She said the station was evacuated, but the whole incident was over in about 1 hour. The envelope was addressed to the secretary, the sergeant said, adding nothing about the envelope was menacing. Source: http://www.scpr.org/news/2010/09/28/suspicious-envelope-prompts-evacuation-lapd-statio/

Energy

Pipeline control room workers focus of safety concerns. The San Bruno, California natural gas explosion that killed 8 people and destroyed dozens of homes has underscored a growing concern about the capabilities of utility employees who watch over the nation's pipelines and whose errors have been linked to many mishaps, some of them catastrophic. The National Transportation and Safety Board (NTSB) has said it is reviewing whether workers at a PG&E pipeline-monitoring terminal in Milpitas were fatigued or poorly trained. And just 8 days after the September 9 blast, the federal Pipeline and Hazardous Materials Safety Administration (PHMSA) moved to speed up adoption of a rule to insure workers are well-trained and rested — especially since many put in 12-hour shifts. Making sure utility employees aren't too tired or otherwise incapable of managing the computerized data they see is essential, said the president of Houston-based Consipio, which advises gas companies on such matters. A 2005 NTSB study that scrutinized 13 pipeline mishaps involving various liquids from 1992 to 2004 found problems were aggravated when workers monitoring the systems failed to quickly recognize and respond to leaks. And from 1990 to 2009, gas-line operator errors caused a little more than 5 percent of all significant accidents nationwide, resulting in 8 fatalities, 150 injuries and $16.2 million in property damage, according to PHMSA data. During the same period, operator error caused 11.5 percent of "serious incidents," which involve a fatality or an injury requiring hospitalization. Source:
http://www.mercurynews.com/news/ci_16230206?source=rss&nclick_check=1

Stuxnet attack exposes inherent problems in power grid security. Power companies and organizations that run supervisory control and data acquisition (SCADA) and process control systems face challenges securing this traditionally proprietary technology. Many of these products have been known to carry vulnerabilities for years, and typical security tools can not drill down into this often-closed software, said the CSO for NetWitness, a founding member of the Energy Sec interest group, where power companies swap threat information. If they are hit with malware, there must be a way to catch it, he said. "A lot of the industry unfortunately is still based on old-style serial interfaces" for communication. The SCADA and power industry will have to follow what retail did with its old POS systems when PCI hit and they needed security. "They suddenly had to implement security ... and some of the interfaces were serial or other types of things that complicated matters," the CSO said. The director of critical infrastructure markets for NitroSecurity agreed that access to PLCs is needed to secure them properly. Source:
http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=227500817

DOE awards $30 million to bolster smart grid cybersecurity. Speaking at the first GridWise Global Forum, the U.S. Energy Secretary last week announced the investment of more than $30 million for 10 projects that will address cybersecurity issues facing the U.S. electric grid. Together, the projects represent a significant investment in addressing cybersecurity issues in the nation's electric infrastructure. The Department of Energy's selections address cybersecurity concerns from two approaches: 1) research and development on innovative cybersecurity solutions, and 2) the establishment of the National Electric Sector Cybersecurity Organization. Innovative Cybersecurity Solutions — $20 million. Source: http://homelandsecuritynewswire.com/doe-awards-30-million-bolster-smart-grid-cybersecurity

Food and Agriculture

(Iowa; Nebraska; Oklahoma) **Oklahoma salmonella outbreak grows.** The Oklahoma salmonella outbreak has risen to 15 identified cases in three counties. The state health department's investigation also determined the outbreak may extend into Nebraska and Iowa. The department is monitoring the outbreak of a similar strain of salmonella identified in the other two states, said the Oklahoma Health Department's communicable disease division director. Two additional cases were identified October 1 among elementary-age children in the Mustang School District in Canadian County, for a total of 12 cases there. Also previously confirmed were two adult cases in Oklahoma County, including one person hospitalized. Carter County also has a young adult with a confirmed case of salmonella. So far, they have not been able to identify sources or possible sources of the bacterial disease. It appears that not all the Oklahoma cases are tied to the school system. The source could be food that is widely distributed to several areas of the state, the communicable disease division director said, but there's not enough information yet to suggest a food that people should avoid. Source: http://newsok.com/salmonella-outbreak-spreads-in-oklahoma/article/3500754

(New York) **Manhattan firm recalling tainted soybean sprouts.** A New York City, New York firm is recalling packages of soybean sprouts after routine sampling by state inspectors detected the presence of listeria. The New York State agriculture commissioner September 30 said the recalled soybean sprouts were sold only by Essex Farm Inc. located inside the Essex Street Market at 120 Essex St. He said the sprouts were marketed on random weight plastic foam trays overwrapped with clear plastic and were not coded. They were sold only at the Manhattan location. Customers who purchased the soybean sprouts from Essex Farm are urged to return them to the market or to discard them. Source: http://www.cnbc.com/id/39451647

(Ohio) **Sandusky County reports case of Eastern equine encephalitis.** A case of Eastern equine encephalitis has been confirmed in the death of a horse on a farm in Sandusky County, Ohio, the Sandusky County Health Department reported September 28. The disease, commonly called sleeping sickness, can be spread to humans, according to the report, though there are no known human illnesses associated with this confirmation of the disease. There have been occasional cases of the disease in Ohio since a large outbreak occurred in horses in 1991 in Wayne and Holmes counties. The disease is caused by a virus that can infect birds, horses and humans, the department reported, and is transmitted by mosquitoes. Source: http://www.thenews-messenger.com/article/20101001/NEWS01/10010311/Horse-dies-of-mosquito-transmitted-disease

(Nevada) **Audit: Agriculture Department failed to make inspections.** The Nevada Department of Agriculture is required to inspect and test commercial fertilizers to determine if they are safe. According to an audit, the department received $416,000 during fiscal 2008 and 2009 but never performed the required inspections. The department also collected $26,000 in fees for the inspection of antifreeze but failed to carry out its duties. The legislative audit said the testing and analysis of commercial fertilizers is important for the protection of public health and safety, domestic animals, and the environment. It said fertilizers often contain concentrations of hazardous materials such as arsenic, mercury, and lead. The inspection of antifreeze determines if the products meet standards for corrosion, freezing, and boiling points, the audit said. The agriculture director said the tests were not conducted due to higher priorities, staff turnover, and recent staff reductions. He said he has recently hired a chemist to do these inspections, which will start this fiscal year. Source:

http://www.lasvegassun.com/news/2010/sep/29/audit-agriculture-department-failed-make-inspectio/

(Kansas; Nebraska; Iowa) **Cattle producers urged to watch for Anaplasmosis.** A seasonal spike in the deadly cattle disease Anaplasmosis has been reported in Kansas, Nebraska and Iowa, and a Kansas State University (KSU) veterinarian is encouraging producers to be vigilant in monitoring cattle. "It occurs almost exclusively in adult cattle," a KSU Research and Extension veterinarian said. "The most frequent observation is sudden death, even though it actually takes a few days from the time signs first appear until death occurs." Early symptoms include white skin that appears yellow and whites of the eyes that will also appear yellow, he said, and dairy cows will drop in lactation. "Treatment with a long-acting oxytetracycline (LA-200 type products) will usually stop further death losses within a week following treatment," he added. "However, producers should be careful as the simple exertion caused by driving cattle to or working them through the chute may be enough to kill more severely affected ones. Most producers who have been feeding chlortetracycline this summer (CTC or Aureomycin) will not have the problem. CTC feeding should continue until the end of fly season." Source: http://wisconsinagconnection.com/story-regional.php?tble=IA2010&ID=952

(Kansas) **State of Kansas gets $1.1 million federal grant to improve livestock feed inspection.** Kansas is receiving a $1.1 million federal grant to improve its efforts to keep animal feed safe. The state department of agriculture announced the grant September 27 from the U.S. Food and Drug Administration. The state agency will use part of the money for 50 additional inspections each year of companies that make, distribute or transport animal feed. It now does 287 inspections annually. The inspections are designed to make sure the feed is free of materials that could lead to mad cow disease. Also, the Kansas agriculture department said the grant would allow it to replace aging lab equipment used to test grain feed for toxins caused by mold. Source: http://www.kansascity.com/2010/09/27/2255989/state-of-kansas-gets-11-million.html

(Wisconsin) **State meat plant recalling cured uncooked sausage.** Mekong Fresh Meats in Mosinee, Wisconsin, is recalling nearly 30,000 pounds of cured uncooked pork ginger sausages because they contain an undeclared allergen "wheat," the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service announced. Each package bears the establishment number "EST. 27488A" inside the USDA mark of inspection. The sausage products were produced between June 21 and September 21. These products were distributed to retail establishments in Alaska, Arkansas, California, Colorado, Georgia, Michigan, Minnesota, Missouri, North Carolina, Ohio, Oklahoma, and Wisconsin. Source: http://www.wisconsinagconnection.com/story-state.php?Id=1131&yr=2010

Government Sector (including Schools and Universities)

3 grenades explode near U.S. Consulate. Three grenades were set off near the U.S. Consulate in Monterrey, Mexico, October 1, one of them only 44 yards away, a staffer said. A duty officer at the consulate in Mexico's third-largest metropolitan area said the first explosion was heard about 8 p.m. There were two more blasts within 1 hour. The duty officer said the explosions did some damage to nearby cars, but there were no reports of any U.S. citizens being injured or suffering property loss. The consulate is in a neighborhood filled with government buildings, the El Norte newspaper said. One grenade went off near the courthouse, injuring a night watchman who was hit by shrapnel, while

another was set off near a prison. The duty officer said none of the grenades appeared to be aimed at the consulate, which remains open. He said U.S. officials are cooperating with Mexican investigators. Source: http://www.upi.com/Top_News/US/2010/10/02/3-grenades-explode-near-US-Consulate/UPI-16341286072682/

GSA puts cyber focus on control systems. The General Services Administration (GSA) will mandate better cybersecurity for control systems in buildings owned by the Public Building Service (PBS). More than 1,500 facilities across the country will have to take specific steps to better protect an assortment of systems connected to the Internet or require connectivity that manage the buildings critical functions from air conditioning to power supply. A draft memo obtained by Federal News Radio lays out the nine steps GSA is requiring. "This is intended to be a high level policy statement that 'stops the bleeding' regarding installing building system networks that do not meet GSA IT/security requirements," the draft policy states. "This issuance establishes PBS policy to meet federal and GSA information security policies and standards for the integration of network based building systems to achieve a consistent agency-wide approach. This policy clarifies the roles and responsibilities of the various PBS Offices and simplifies the integration of information technology into PBS-owned building information or control systems." The policy is effective October 1. Source: http://www.federalnewsradio.com/index.php?nid=35&sid=2066346

(Ohio) **Daycare threats under investigation in Ohio.** Two federal agencies — the FBI and the U.S. Postal Service — are investigating threatening letters that have been sent to at least two KinderCare facilities in Ohio. A spokesman for the Cincinnati office of the FBI confirmed an investigation October 1, but divulged no specifics about the alleged threats, including which daycares are involved or the total number. "We don't see an imminent threat as a result of the letters," the spokesman said. Various media reports place it at three — two in Butler County and one in Montgomery County near Dayton. On September 10, Fairfield Township police said security was heightened at the Morris Road KinderCare facility after it received a threatening letter written by a person who "felt that everyone at Kinder Care should die in a 9/11-style attack." On September 30, KinderCare Learning Center at 1250 Elliott Dr. in Middletown told at least two media outlets it received a similar letter. Middletown police said October 1 they had no information about such an incident. Source: http://news.cincinnati.com/article/20101001/NEWS010701/310010005/Daycares-get-terror-threats

Deloitte/NASCIO Survey: Government data and citizens' personal information at risk. According to findings of a recent survey conducted by Deloitte and the National Association of State Chief Information Officers (NASCIO), "State Governments at risk: A Call to Secure Citizen Data and Inspire Public Trust," state governments, as custodians of the most comprehensive collection of citizens' Personally Identifiable Information (PII), must make cybersecurity a top priority. The study finds that many state Chief Information Security Officers (CISOs) lack the funding, programs and resources to adequately protect vital government data and the personal information of their constituents, especially when compared to their counterparts in private sector enterprises. "Many state CISOs lack the visibility and authority to effectively drive security down to the individual agency level," said the director, Deloitte & Touche LLP and leader of state government security and privacy services. "At the federal level, the President has recognized the critical nature of the problem and appointed a cybersecurity coordinator to address it; it's imperative that governors and state legislative leaders make cybersecurity a priority." "Unprecedented budgetary cuts across state governments and growing reliance on contractors and outsourced IT services are creating an environment that is even

harder to secure," said the president of NASCIO and CIO for Utah. The study is based on a survey responses from 49 of the 50 states. Source: http://www.darkreading.com/database_security/security/government/showArticle.jhtml?articleID=227500972&subSection=End+user/client+security

(Florida) **Driver in custody after bomb scare at Cape Canaveral Air Force Station.** A man was taken into Baker Act custody after he tried to enter Cape Canaveral Air Force Station in Florida September 27 while driving a van reported to be carrying suspicious goods. Inside the vehicle, the Brevard County Sheriff's Office bomb squad found a briefcase, motor oil, and antifreeze, officials said. "They didn't find anything dangerous on him," said a spokesman for the 45th Space Wing. "But he was acting strangely." The sheriff's office took the man into custody under the Baker Act, which allows the police to commit individuals to the care of medical professionals against their will. Investigators said the man had contact with people at the Air Force station, but they would not confirm the details of those connections. The incident began about 9 a.m. outside Gate 1, the southernmost entrance to the base on State Road 401. Though the van was beyond the station's fence line, it did not reach the gate. Source: http://www.floridatoday.com/article/20100928/NEWS01/9280320/1006/Driver+in+custody+after+bomb+scare+at+Cape+Canaveral+Air+Force+Station

(Texas) **Shots fired at University of Texas Austin, cops hunt possible second suspect.** A gunman wearing a ski mask and brandishing a rifle entered a library at the University of Texas at Austin September 28 and fired several shots before taking his own life, university officials said. Officials said a suspect brought a semi-automatic gun to the school's library. Police are still looking for a possible second suspect and the campus, site of an infamous 1966 school shooting, remains on lockdown. "The armed suspect is dead. No other injuries have been reported," the university president wrote in a campus e-mail. An e-mail and text alert was sent to students and faculty around 8 a.m., just as the day's first classes were beginning, warning that an "armed subject was reported last seen at Perry Castaneda Library" and telling students to remain in place. Source: http://abcnews.go.com/US/shots-fired-university-texas-austin-cops-hunt-gunman/story?id=11744405

Information Technology and Telecommunications

Trojans made up 55% of all malware in Q3. More than half (55 percent) of all new malware identified in Q3 of this year were Trojan viruses, said PandaLabs. The research arm of Panda Security said most of these were banker trojans designed to trick Web users into navigating to fake financial sites so cybercriminals can steal log-in details and passwords. The use of e-mail in distributing malware, once the most favored method, has declined. Instead, cybercriminals are resorting to social-media-related infections, including clickjacking attacks on social networks such as Facebook, and poisoned search results. Panda also said 95 percent of all e-mail received during Q3 was spam, and 50 percent of this was sent from just 10 countries, which included India, Brazil, and Russia. For the first time, the United Kingdom has fallen out of the list of the world's biggest spam-producing countries. The security firm also said over the past 3 months it has seen a number of attacks on Google Android phones, which could be the beginning of a wave of threats targeting smartphones. Source: http://www.networkworld.com/news/2010/100110-trojans-made-up-55-of.html?hpg1=bn

IE users most at risk from DLL hijacking attacks. Users of Microsoft's Internet Explorer (IE) are more vulnerable to rogue DLL attacks than people who use rival browsers such as Mozilla's Firefox or Google's Chrome, a security researcher said September 29. When running on Windows XP, IE6, IE7, and IE8 do not warn users when they click on a malicious link that automatically downloads a malicious dynamic link library, or DLL, to the PC, said the CEO of Slovenian security company Acros Security. Users running IE7 or IE8 on Windows Vista or Windows 7 are safer, said the researcher, who noted that both browsers run by default in "Protected Mode" on those operating systems. The problem on XP is that it automatically opens Windows Explorer, the operating system's file manager, whenever IE encounters a remote shared folder. "It's not so much that IE itself is vulnerable to binary planting, but that other applications' binary planting vulnerabilities can be exploited relatively easily through IE, and in most cases without a single warning," the researcher said. Source: http://www.computerworld.com/s/article/9188779/IE_users_most_at_risk_from_DLL_hijacking_attacks

Phishers target WoW players through in-game mail system. Security researchers from Trend Micro warn that World of Warcraft (Wow) players are being targeted through the game's internal mail system by phishers looking to steal their Battle.net credentials. Rogue chat messages (whispers) have been used to direct players to phishing pages for a while now, but Trend Micro researchers warn that attackers are increasingly impersonating game administrators. The messages attempt to scare users into thinking that there is something wrong with their account and they risk getting suspended unless they log into a Web site and perform a special action. However, the mail system has also begun being abused by phishers. "In this new trickery, the phishing URLs are sent via WoW in-game mail and is received by players in their in-game mailboxes," the solutions product manager at Trend warned. "The mail message is full of a mix of surprises. It combines several elements from other Blizzard games. [â¦] To add to its credibility, the phishing URL contains the string worldofwarcraft and an abbreviation of Cataclysm," he explained. Source: http://news.softpedia.com/news/Phishers-Target-WoW-Players-Through-In-Game-Mail-System-158654.shtml

XSS worm hits Orkut. A cross-site scripting vulnerability was exploited September 25 on Orkut to launch a fast-spreading worm that auto-posted a rogue message reading "Bom Sabado" on people's scrapbooks. "Bom Sabado" means "Good Saturday" in Portuguese, which led some people to assume that the worm originated in Brazil, where Orkut has a significantly large user base. The messages, which has rogue JavaScript code embedded into them, forced logged in users to repost them on their friends' scrapbooks (the equivalent of "Walls" on Facebook). The attack was extremely viral and affected almost 10 percent of all Orkut users, 70 percent of whom are from India or Brazil. The social network has over 52 million users. Google fixed the underlying vulnerability in a matter of hours. According to some reports, the worm also automatically subscribed victims to a group. However, News Live quotes a Google spokesperson who said the attack was not malicious. Source: http://news.softpedia.com/news/XSS-Worm-Hits-Orkut-158198.shtml

Many Android apps leak user privacy data. A recent test of prototype security code for Android phones found that 15 of 30 free Android Market applications sent users' private information to remote advertising servers, without the users being aware of what was being sent or to whom. In some cases, the user's location data was sent as often as every 30 seconds. The software, called TaintDroid, was designed to uncover how user-permitted applications actually access and use private or sensitive data, including location, phone numbers, and even SIM card identifiers, and to notify

users within seconds. The findings suggest that Android, and other phone operating systems, need to do more to monitor what third-party applications are doing under the covers of smartphones. TaintDroid is a joint effort by researchers at Duke University, Intel Labs, and Penn State University. The team's paper, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones" will be presented in October at the USENIX Symposium on Operating Systems Design and Implementation. Source: http://www.networkworld.com/news/2010/092910-android-privacy.html

Google warns Gmail users on spying attempts from China. Recently, a number of users have been witnessing a glaring red banner popping up when they accessed their Gmail account, saying "Warning: We believe your account was recently accessed from: China (IP ADDRESS)". ThreatPost reports that among the seemingly random victims — gamers, doctors, media consultants — was also a member of Privacy International in the United Kingdom. Even though his Gmail account is wholly unconnected with his work for the human rights organization, he said that it is possible that he was targeted because of a EU-China Human Rights Network seminar during which he discussed freedom of speech issues and differences between the EU and China on that account. All users who have been similarly warned are advised by Google to change their passwords. Technolog asked Google to comment on the occurrence, and they said that the banner is simply part of the security feature introduced in March. Source: http://www.net-security.org/secworld.php?id=9917

U.S. leads the way in malware and firewall attacks. The United States has overtaken India and Russia to become the biggest producer of viruses once more, according to Network Box. The United States is now responsible for 12 percent of the world's viruses, up from 4 percent from August, when the United States trailed both India and Russia. India takes second place with 7.17 percent, after its virus production declined by 6.56 percent. Russia, which was in third place, has dropped to fifth after a fall of 5.53 percent, to be replaced by Korea, which saw an increase in production of 0.27 percent (reaching 6.29 percent of virus production). Viruses produced in the United Kingdom have dropped again (by 0.29 percent). The United Kingdom has now dropped from fourth largest producer in July, to tenth in September. The United States and India still dominate when it comes to spam production, being responsible for 10.79 and 6.88 percent of the world's spam, respectively. Russia has replaced Brazil as the third largest spam producer, after an increase of 2.53 percent from last month, to 6.04 percent of the world's spam. The majority of firewall attacks still originate from the United States (18.65 percent) — in fact there was a slight increase of 0.32 percent in September. Source: http://www.net-security.org/malware_news.php?id=1473

National Monuments and Icons

(Oklahoma) **Fire destroys barracks at historic Fort Washita.** The replica of a military barracks at Fort Washita in southeastern Oklahoma was destroyed by fire about 7:30 a.m. September 26. The state fire marshal's office is looking for the cause of the blaze. The site is near Durant — about 135 miles southeast of Oklahoma City. It was established in 1842 as a military fort. The site was acquired by the Oklahoma Historical Society in 1962 and the barracks were built in 1972. It was designated a National Historic Location in 1965. The park superintendent estimated the damage at $2 million. Source: http://www.kswo.com/Global/story.asp?S=13222724

(Wyoming) **Antelope Fire in Yellowstone reaches 3,000+ acres, 50 percent containment.** The Antelope Fire, Yellowstone National Park's largest fire this year, has grown to 3,072 acres and is 50 percent contained. The park issued a final report on the fire September 26, unless any significant activity occurs. Small spots of smoldering vegetation were observed within the interior of the burned area. Helicopter water drops cooled isolated torching of small trees and fire that had creeped into the grass in the southeastern corner, the park said. "The Antelope fire is helping Yellowstone achieve its fire and resource management goals. It has provided a new fuels buffer that will increase the defensibility of the Tower developments in the event of future fires in the Mount Washburn area," the park said. "Yellowstone National Park is a fire adapted ecosystem, and fire plays an important role in maintaining the health of the area's wildlife habitat and vegetation." Source: http://www.kxlf.com/news/antelope-fire-in-yellowstone-reaches-3-000-acres-50-percent-containment/

Postal and Shipping

(Alaska) **Downtown business owner finds strange substance in letter.** A Juneau, Alaska business owner reported receiving a pair of strange letters, one containing an unknown substance, to the Juneau Police Department (JPD), according to a press release from JPD. The business owner called police the morning of October 4 to report the letters, the release states. JPD and Capital City Fire and Rescue's Hazardous Materials team responded and took possession of both letters. The FBI has been notified, according to the release, and the materials will be shipped to a testing lab to identify the substance. Source: http://www.juneauempire.com/stories/100110/reg_714443592.shtml

(Alabama) **Suspicious package reported in Homewood.** Homewood, Alabama Fire and Rescue reported with the HAZMAT unit to the Alabama Republican Party's office in Homewood after dispatch received a call about a suspicious package. There was a white substance in the package, but it has not been identified. The contents will be mailed to a state lab in Montgomery for analysis. The occupants of the building, including rescue personnel, underwent decontamination. The Alabama Bureau of Investigation, Homewood Police, and FBI are involved in the investigation. Source: http://www.myfoxal.com/Global/story.asp?S=13233718

Public Health

(California) **Bomb threat at sober living center leads to evacuation.** A phoned-in bomb threat about 2 p.m. October 3 prompted police to order the evacuation of the Beit T'Shuvah sober living facility on Venice Boulevard in West Los Angeles, California. Residents waited 1 block away for more than 1 hour as Los Angeles police officers searched the building. Police diverted traffic on Venice between Helms Avenue and National Boulevard. Dozens of furniture shoppers in Culver City's Helms Bakery District across the street were ordered to stay inside the stores. Officers gave the all clear just before 4 p.m., and residents returned to the sober living facility. Source: http://latimesblogs.latimes.com/lanow/2010/10/bomb-threat-leads-to-sober-living-center-evacuation.html

Identifying enzymes to explode superbugs. A group of U.S. researchers has developed a method that can identify enzymes for optimum bacteria-killing characteristics to kill antibiotic-resistant superbugs like Methicillin-resistant Staphylococcus aureus or MRSA. A paper published October 4 in IOP

Publishing's Physical Biology, shows how lytic enzymes can be used to attack bacteria by piercing their cell walls. Lytic enzymes are proteins that are naturally present in viruses, bacteria and in body fluids such as tears, saliva and mucus. However, until now, largely ad-hoc methods have been used to calculate the enzymes' killing abilities. The researchers in the new study, including two quantitative biologists at the Georgia Institute of Technology and a biochemist from the University of Maryland, found that most lytic enzymes kill only a limited range of bacteria, unlike antibiotics, which allows them to target superbugs while potentially leaving beneficial bacteria intact. Source: http://www.eurekalert.org/pub_releases/2010-10/iop-iet100310.php

(Nebraska) **Shooting tests hospital security.** Hospitals are wide-open places featuring life-and-death drama and intense emotion, and in rare instances those factors lead to violence. A man was killed September 29 at Creighton University Medical Center in Omaha, Nebraska after he fired a handgun at police officers in the hospital. He was fatally wounded by return fire. Although he may have intended to target his mother-in-law, who works at the Boys Town National Research Hospital adjacent to the medical center, the incident raises security questions about hospitals, and trauma centers in particular. Trauma centers are formally designated to treat gunshot victims, auto-wreck victims and others suffering severe injuries. The Creighton hospital and the Nebraska Medical Center are Omaha's trauma centers, and BryanLGH Medical Center West is Lincoln's. Source: http://www.omaha.com/article/20101001/NEWS97/710019871/0

HHS Centers of Innovation to Speed Vaccines. The Department of Health and Human Services (HHS) has released a draft solicitation to the biomedical industry for the creation of centers of innovation for speedy development and manufacture of advanced medical countermeasures. The goal of the September 15 draft is to stand up a flexible platform for producing medical countermeasures for a variety of biological threats, a HHS secretary stressed in testimony before the Senate Appropriations Committee. Such innovation centers would provide a surge capacity for the production of flu vaccine, as necessary, but they also would have "the ability to mix and match and to respond to something that we don't know is coming," she said. The centers could produce countermeasures in the face of a bioterrorism attack that utilized anthrax or other infectious biological agents. Source: http://www.hstoday.us/content/view/14909/128/

Social networks for patients stir privacy, security worries. Social networking is infiltrating healthcare with platforms for patients to share intimate details of their diagnoses, medications, physical conditions, locations, and other personal data — and not necessarily anonymously. Members of emerging sites, such as PatientsLikeMe, DailyStrength, and HealthyPlace, for example, can post profiles similar to those on Facebook, and many users are posting their photos, hometowns, and personal health information that could ultimately be abused. And like mainstream social networks Facebook and LinkedIn, these online patient communities are attractive targets for identity thieves, spammers, and other bad guys trolling for valuable information, security experts said. They also could be used for targeted attacks, or by employers, or other people to gather private information about the patient that could be used against her. Ironically, the emergence of these sites comes amid growing concerns over patient privacy and security of their data in the move to electronic medical records. Source: http://www.darkreading.com/authentication/security/privacy/showArticle.jhtml?articleID=227500908

Swine flu no longer a major threat to USA. Swine flu no longer represents a major threat to the U.S. population, because most people are immune to the virus that caused last season's pandemic, health officials reported September 28. Of the 310 million people in the United States, 59 percent are now believed to be immune to pandemic H1N1 flu, the researchers said. Approximately 62 million people were vaccinated against the virus, 61 million people were infected by it, and another 60 million people 57 or older carry protective antibodies against similar viruses that date back to previous pandemics. "It's very unlikely that the virus will explode in the fall," said the director of the National Institute of Allergy and Infectious Diseases (NIAID), an author of the analysis. "We now have evidence of that." The evidence comes from studies on the 2009-2010 pandemic carried out by the Centers for Disease Control and Prevention. If this virus follows the pattern set by earlier flu bugs, it will either die out completely or continue to circulate in the ever-shrinking pool of people still susceptible to it, the authors reported in the journal mBio. Source: http://www.usatoday.com/yourlife/health/medical/coldflu/2010-09-29-flufate29_ST_N.htm

TRANSPORTATION

Airport lobbies possible terror targets in European plot, official says. Among the possible targets in the suspected European terror plot are pre-security areas in at least five major European airports, a law enforcement official said. Authorities believe terror teams are preparing to mount a commando like attack featuring small units and small firearms modeled after the Mumbai, India attack 2 years ago. The U.S. State Department issued a highly unusual "Travel Alert" October 3 for "potential terrorist attacks in Europe," saying U.S. citizens are "reminded of the potential for terrorists to attack public transportation systems and other tourist infrastructure." One scenario authorities fear is a repeat of the 1985 attack on the Rome and Vienna airports, when Palestinian extremists threw grenades and opened fire on travelers waiting at ticket counters injuring 140 and killing 19. European and U.S. officials first learned of the current terror threat over the summer following the capture of a suspected German terrorist who had been training in Pakistan. The plot's leaders have been identified and targeted, Pakistan's ambassador said October 3. A curfew was ordered this weekend at Ramstein U.S. Air Force Base in Germany, with soldiers told to remain at home and not to wear uniforms off base "in response to a threat condition," a Ramstein spokesperson said. Source: http://abcnews.go.com/print?id=11790782

(Kentucky) **Man convicted of stealing copper from rail shop faces 20 years.** A western Kentucky jury has convicted a former security guard of stealing copper cable at a railroad engine shop in Paducah where he formerly worked. The jury recommended a maximum 20-year prison term. The man caused more than $500,000 damage to 34 railroad engines by cutting copper cabling out of them while they were at VMW Paducahbilt to be overhauled. The Kentucky commonwealth's attorney said the company also reported up to $500,000 more in lost business because of the damage. Source: http://www.kentucky.com/2010/09/29/1456016/man-convicted-of-stealing-copper.html

Gels, liquids may be allowed back onto planes by 2012. Airline passengers may once again be allowed to board flights with creams, gels and liquids that were banned over security concerns, the International Civil Aviation Organization said September 27. "In the next two years (the ban) will end," the ICAO Secretary General told AFP ahead of the UN organization's 37th general assembly. New equipment capable of detecting explosives in water bottles, makeup kits or toothpaste tubes, for example, would be installed at most airport security checkpoints by 2012, he explained. The

unprecedented security measure took effect in 2006 after British police foiled a transatlantic plot to detonate liquid explosives aboard airliners flying to Canada and the United States. Controversial full body scanners, opposed by nations including Italy, will still be used to varying degrees in the short term because they allow for quicker inspections and reduce lines at airport security checkpoints. Source: http://www.google.com/hostednews/afp/article/ALeqM5jW79YzpxBemb4fv5EIBxxMYUKjhw?docId=CNG.4c0adf87019fdcb41173c1f2f50269df.6e1

(New York) **MTA unveils subway emergency intercom.** Deep underground on a subway platform with no cell phone service or station agent in sight, reporting an emergency can be difficult. New York City's Metropolitan Transportation Authority (MTA) highlighted a new intercom device that would help alert transit workers in seconds. The intercoms offer emergency assistance or travel information with the push of a button. The intercoms are highly visible, unlike the current call boxes, and they instantly give one's exact location. They can also be equipped with cameras. One of the first help point intercoms will be introduced at the 23rd Street and Lexington Avenue subway station in November. The goal is to have them in all stations citywide in 2 years. Source: http://www.myfoxny.com/dpp/traffic/mta/mta-unveils-subway-emergency-intercom-20100927

(Nebraska) **Bomb squad responds to suspicious device on UP Railroad property.** Officials are investigating after a suspicious device was found on Union Pacific Railroad (UP) property in Nebraska, September 27. The device was found about 1:30 p.m. on UP property about 8 miles east of Cozad, according to a press release from the Dawson County Sheriff's Office. The Nebraska State Patrol was called, and the destructive device was made safe by a bomb technician of the Nebraska State Patrol bomb squad. The Lexington Volunteer Fire and Rescue Department was standing by at the scene. The Federal Bureau of Investigation, Union Pacific Railroad Police Department, Nebraska State Patrol and Dawson County Sheriff's Office are investigating the incident. Source: http://www.kearneyhub.com/news/local/article_6e4c38e0-cb02-11df-ac96-001cc4c002e0.html

Water and Dams

Metal thieves damage Bishop Auckland flood defence. Thieves hunting for scrap metal have been blamed for damaging a County Durham, England, flood defense. The Environment Agency's 8.8 million pound Spring Gardens dam protects 660 properties in Bishop Auckland from flooding from the River Gaunless. It said metal hinges and catches from the gate of the dam had been removed with the cost of the damage put at 3,000 pounds. It is urging people to be vigilant and report any dam damage. The agency operations delivery team leader said, "I'm shocked that people would put others in danger to steal hinges which are probably just sold as scrap." He said metal thieves had targeted the dam before by stealing stainless steel beams, used to regulate the flow of water upstream. The agency is trying to find new parts to carry out the repairs as soon as possible. Source: http://www.bbc.co.uk/news/uk-england-11442385

(Wisconsin) **Flood damage tops $9 million.** Wisconsin State officials want the federal government to assess flood damage next week to see if disaster aid could be available to fix roads and other public facilities. Wisconsin Emergency Management reports the public sector damage from the recent rains and floods surpassed $9 million September 30, and the damage is still being tallied while some spots remain underwater. The only significant flooding October 1 was on the Mississippi River. It was a half

foot over its banks at La Crosse at 2 a.m., and it was still 3.1 ft. above its flood stage at McGregor, Iowa, near Prairie du Chien. The Wisconsin River at Muscoda returned to its flood stage overnight. According to a Wisconsin Department of Natural Resources press release, the water level of the Wisconsin River at Portage continues to drop at the rate of about 1-inch an hour, and officials are hoping the worst is over at the Caledonia-Lewiston Levee, popularly known as the Portage Levee. Source: http://www.rivertowns.net/event/article/id/233414/

Elevated nitrogen and phosphorus still widespread in much of the nation's streams and groundwater. Elevated concentrations of nitrogen and phosphorus, nutrients that can negatively impact aquatic ecosystems and human health, have remained the same or increased in many streams and aquifers across the United States since the early 1990's, according to a new study by the U.S.Geological Survey (USGS). "This report provides the most comprehensive national-scale assessment to date of nitrogen and phosphorus in our streams and groundwater," said the USGS director. USGS findings show that widespread concentrations of nitrogen and phosphorus remain two to ten times greater than levels recommended by the EPA to protect aquatic life. Most often, these elevated levels were found in agricultural and urban streams. These findings show that continued reductions in nutrient sources and implementation of land-management strategies for reducing nutrient delivery to streams are needed to meet EPA recommended levels in most regions. The study also found that nitrate is a continuing human-health concern in many shallow aquifers that are sources of drinking water. Source: http://www.pollutiononline.com/article.mvc/Elevated-Nitrogen-And-Phosphorus-Still-0001?VNETCOOKIE=NO

Worldwide groundwater depletion rate accelerating. In recent decades, the rate at which humans worldwide are pumping dry the vast underground stores of water that billions depend on has more than doubled, said scientists who have conducted an unusual, global assessment of groundwater use and recently released results of their study. These fast-shrinking subterranean reservoirs are essential to daily life and agriculture in many regions, while also sustaining streams, wetlands, and ecosystems and resisting land subsidence and salt water intrusion into fresh water supplies. Today, people are drawing so much water from below that they are adding enough of it to the oceans (mainly by evaporation, then precipitation) to account for about 25 percent of the annual sea level rise across the planet, the researchers found. Soaring global groundwater depletion bodes a potential disaster for an increasingly globalized agricultural system, said a researcher of Utrecht University in Utrecht, the Netherlands, and leader of the new study. He and his colleagues will publish their new findings in an upcoming issue of Geophysical Research Letters, a journal of the American Geophysical Union. In the new study, which compares estimates of groundwater added by rain and other sources to the amounts being removed for agriculture and other uses, the team taps a database of global groundwater information including maps of groundwater regions and water demand. Source: http://homelandsecuritynewswire.com/worldwide-groundwater-depletion-rate-accelerating

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**